

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
GREENVILLE DIVISION

KYLE KEOGH, on behalf of himself and all others
similarly situated,

Plaintiff,

v.

META PLATFORMS, INC.,

Defendant.

Case No. 6:23-cv-5004-KDB

**PLAINTIFF’S RESPONSE IN OPPOSITION TO DEFENDANT
META PLATFORMS, INC.’S MOTION TO DISMISS**

I. INTRODUCTION

Almost every argument Defendant Meta Platforms, Inc. (“Meta”) raises in its motion to dismiss this case has already been rejected by the court in *Gershzon v. Meta Platforms, Inc.*, 2023 WL 5420234 (N.D. Cal. Aug. 22, 2023), which denied Meta’s motion to dismiss another class action based on its Tracking Pixel obtaining and using personal information from the California DMV website. Similar to *Gershzon*, this is a class action suit brought against Defendant Meta Platforms, Inc. (“Meta”) for covertly tracking South Carolinians’ personal records including permanent disability placard renewals, new car registrations, identification card renewals, and other activity on the South Carolina Department of Motor Vehicles (“DMV”) website. The crux of this case rests on the simple fact that neither Meta nor the DMV asked South Carolina drivers for their express written consent to obtain or use this highly sensitive information for advertising, and by doing so, Meta violated the federal Drivers’ Privacy Protection Act, 18 U.S.C. § 2721, et seq. (“DPPA”). Given the similar stance of Plaintiffs, Meta’s motion here should be denied for many of the same reasons set forth in *Gershzon*.

II. ARGUMENT

A. **Meta Obtained “Personal Information From A Motor Vehicle Record”**

Meta’s main argument – that it never “received any identifying information ‘from a motor vehicle record’” – repeatedly conflates the concepts of cookies, websites, and web browsers. *See* MTD 7-10; *see also Gershzon*, 2023 WL 5420234, at *7-*8 (rejecting these same arguments). But the allegations here are simple; one need not possess a computer science degree to understand them. First, Mr. Keogh alleges that the South Carolina DMV website is a “motor vehicle record.” Complaint, ¶ 58. Second, this website created cookies containing his Facebook ID number, which is “personal information” that is publicly tied to his real name and identity. *Id.* at ¶¶ 27, 31, 37, and 57. And third, the Meta Tracking Pixel compelled Mr. Keogh’s web browser to transmit these cookies from the South Carolina DMV website to Meta’s website, facebook.com. *Id.* at ¶ 27.

Mr. Keogh will address each of these contentions in turn.

1. ***The South Carolina DMV Website Is A Motor Vehicle Record***

“Webpages on the South Carolina DMV website are a type of ‘motor vehicle record’ within the ambit of the DPPA.” Complaint, ¶ 58; *accord Gershzon*, 2023 WL 5420234, at *8 (where a plaintiff “alleges that Meta obtained his personal information from the DMV website” that is, “sufficient to show that Meta obtained [plaintiff]’s information ‘from a motor vehicle record’”).

Under the DPPA, a “‘motor vehicle record’ means any record that pertains to a motor vehicle operator’s permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.” 18 U.S.C. § 2725(1). The South Carolina DMV

website is “record” because it is “something that records” information. *See Record, Merriam-Webster Online Dictionary* (2023) (defining a “record” as “something that records”).

The South Carolina DMV website records information that “pertain[s] to a motor vehicle operator’s permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.” The complaint includes several screenshots from the DMV website showing the site allows South Carolinians to schedule driving tests, book appointments for new car registrations, or apply for disability placards to place on their cars. *See Compl.*, at Figs. 1, 2, 5; *see also id.* at ¶¶ 1, 3, 20, 22, 24, 26, 43. And the PageView, microdata, and button click events Meta obtains from the South Carolina DMV website tell Meta an enormous trove of sensitive information about South Carolina drivers, such as whether a particular person wishes to schedule a driving test or believes he or she is disabled and applies for a disability placard. *See, e.g., id.* Figs. 3 and 7 (reproduced below).



Meta cites *Lake v. Neal*, 585 F.3d 1059 (7th Cir. 2009), a case involving *voter registration forms*, to argue that the South Carolina DMV website is not a motor vehicle record. MTD at 8. But this case was already found to be unhelpful and inapplicable by the *Gershzon* court:

Lake does not aid Meta. Unlike a voter registration form, a disability parking placard (and an application for such a placard) does pertain to a motor vehicle operator's permit. If a person with a disability is licensed to drive in California and requires an accommodation in the form of a disabled parking placard, the person must apply for such a placard. Disability parking placards are only used in connection with driving, unlike a voter registration form which has no connection to driving. Thus, a disabled parking placard pertains to a motor vehicle operator's permit.

Gershzon, 2023 WL 5420234, at *8.

The same is true of webpages to schedule driving tests or appointments for new car registrations. Indeed, a person needs to complete a driving test to receive “a vehicle operators’ permit” and likewise needs to register a new car to lawfully drive it. Indeed, every single webpage on the South Carolina Department of Motor Vehicles website has some kind of a “connection with driving.” *Gershzon*, 2023 WL 5420234, at *8.

Meta also repeatedly relies on *Andrews v. Sirius XM Radio Inc.*, which held that licenses possessed by drivers were not motor vehicle records because they were not records “*maintained by an agency*” like the DMV. 932 F.3d 1253, 1260 (9th Cir. 2019) (emphasis in original). But “*Andrews*, upon which Meta relies, is factually distinguishable.” *Gershzon*, 2023 WL 5420234, at *8. As *Gershzon* recognized, “[u]nlike *Andrews*, where the defendant obtained personal information from sources other than a DMV, here [plaintiff] alleges that Meta obtained his personal information from the DMV website.” 2023 WL 5420234, at *8. And Meta cannot dispute that the DMV website is “*maintained by*” the DMV.

It is easy to see why *Andrews* has no bearing on this case. In *Andrews*, the plaintiff alleged that, when he purchased a used car, he handed over his driver's license to the car dealership and that dealership, in turn, handed over the information it received from the license

to a subscription-based radio service. 932 F.3d at 1255-56. The Ninth Circuit explained that the DPPA was not meant to cover transactions solely between private actors because “the legislative history and case law [showed] that Congress was motivated to enact the DPPA by ... ‘the States’ common practice of selling personal information to businesses engaged in direct marketing and solicitation.’” *Id.* at 1259-60; *accord* Compl., at ¶¶ 4 and 11. “With this purpose in mind, we interpret” the DPPA as only prohibiting third parties from obtaining or using “‘personal information’ from the DMV’s records.” *Id.* at 1260. And “[a] driver’s license, though issued by the DMV, becomes the possession of *an individual*, not the DMV that issued it.” *Id.* (emphasis in original). To hold otherwise could conceivably “penalize a security guard’s use of a driver’s license photograph” when verifying someone’s age or identity. *Id.* at 1261.

The transaction here is nothing like the provision of a driver’s license on a used car lot. Instead, it is more like a government contractor installing a recording device inside the lobby of the DMV office to surreptitiously record conversations between drivers and DMV staff. Worse yet, Meta installed its Tracking Pixel on the South Carolina DMV website so it could “deliver targeted advertisements to drivers on its social media platforms.” Compl., ¶ 42. This leads to drivers getting pestered with “AAA ad[s] telling them that by joining, they can ‘skip the trip to the DMV’ ... after visiting the South Carolina DMV website.” *Id.* This falls squarely within the class of activity Congress sought to regulate. *See Andrews*, 932 F.3d at 1257 (noting that the DPPA was enacted to stop the “state DMVs’ practice of selling or freely disclosing drivers’ personal information, which led to ... onslaughts of random solicitations”).

2. A Facebook ID Number Is Personal Information

Next, “Facebook ID numbers are ‘personal information,’ within the ambit of the DPPA.” Compl., ¶ 57. Under the DPPA, “personal information” means any “information that identifies

an individual” and expressly includes correlated numbers, such as “[a] social security number, driver identification number, ... [or] telephone number.” 18 U.S.C. § 2725(3). As the court in *Gershzon* acknowledged, “‘personal information’ under the DPPA need only be ‘facts that can identify an individual, as opposed to facts that in every instance must identify an individual.’” *Gershzon*, 2023 WL 5420234, at *6 (citing *United States v. Hastie*, 854 F.3d 1298, 1304 (11th Cir. 2017)). “A Facebook ID allows anybody – not just Facebook – to identify the individual driver with a Facebook account. If one types [www.facebook.com/\[FacebookID\]](http://www.facebook.com/[FacebookID]) a into web browser, it will load that individual’s Facebook page.” Compl., ¶ 28. “Thus, the Facebook ID number is a correlated number – just like a social security number, driver’s license number, or telephone number – which can be used by anyone to identify an individual.” *Id.* at ¶ 29. “A Facebook ID ... is thus equivalent to a name – it stands in for a specific person.” *Robinson v. Disney Online*, 152 F. Supp. 3d 176, 184 (S.D.N.Y. 2015).

Meta also argues that the “Cookies [containing the Facebook ID numbers] ... are created, and subsequently exist, independently of any ‘motor vehicle record.’” MTD at 8. Plaintiff’s counsel fails to see how this matters in the slightest. First and last names, telephone numbers, and social security numbers “are [also] created by, and subsequently exist, independent of any ‘motor vehicle record.’” Our names are usually given to us by our families; our telephone numbers by our phone carriers; our social security numbers by the federal government; all “exist [] independent of any ‘motor vehicle record.’” The DPPA nevertheless *expressly includes* first and last names and telephone and social security numbers in its definition of “personal information.” 18 U.S.C. § 2725(3). It is no surprise then, that *Gershzon* rejected this argument as well. 2023 WL 5420234, at *8. This Court should do the same.

3. *Because Facebook ID Numbers Are “Created By” The South Carolina DMV Website As First-Party Cookies, The Numbers Are “From” A Motor Vehicle Record*

Having established that (1) the South Carolina DMV website is a “motor vehicle record,” and (2) the Facebook ID numbers are “personal information,” the only question left is determining whether the Facebook ID numbers Meta received are *from* the South Carolina DMV website. 18 U.S.C. § 2724(a) (“A person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter ... is liable”). Plaintiff alleges exactly that. Compl., at ¶ 39. (“Meta is collecting a driver[’s] Facebook ID number from the South Carolina DMV website directly”). Again, this very same argument was briefed and rejected in *Gershzon*. 2023 WL 5420234, at *8.

In particular, “[t]he c_user cookie contains that visitor’s unencrypted Facebook ID” and the “fr cookie contains ... an encrypted Facebook ID.” *Id.* at ¶¶ 29 and 32. “Defendant [] obtained and used identifiers for Plaintiff Keogh including the c_user and fr cookies ... as first-party cookies¹ on his web browser.” *Id.* at ¶ 45. “A first-party cookie is ‘created by the website the user is visiting.’”² *Id.* at ¶ 36. Putting this all together, this means that, “by collecting the c_user and fr cookies as first-party cookies, Meta is collecting a driver[’s] Facebook ID number from the South Carolina DMV website directly.” *Id.* at ¶ 39; *see also id.* at ¶ 59; *accord Gershzon*, 2023 WL 5420234, at *2.

¹ By way of background, “Meta introduced first-party cookies in 2018 to allow its tracking Pixel to circumvent improvements in how web browsers block third-party cookies ... a first party cookie became another default [Meta Tracking] Pixel setting in or around October 2018.” *Id.* at ¶ 37; *see also Gershzon*, 2023 WL 5420234, at *2.

² The complaint uses the North Carolina DMV website’s URL as an example, but as noted, it the first party cookies would be created by any website they are placed on. This expressly includes the “first-party cookies... from the South Carolina DMV website.” *Id.* at ¶ 39.

Meta argues dismissal is warranted because the “c_user and fr cookies ... came³ from ‘[Mr. Keogh’s] web browser.’” MTD at 8 (emphasis added). In support of its “came from” argument, Meta cites Mr. Keogh’s allegation that “the DMV website compels a visitor’s browser to transmit an identifying ‘computer cookie’ to Meta called ‘c_user.’” Compl., ¶ 28. But this misses the point. As the Ninth Circuit explained in *Andrews*, the question is whether “the initial source of personal information is a record in the possession of ... a state DMV.” 932 F.3d at 1260 (emphasis added). And here, as alleged, the initial source of the Facebook ID numbers was the South Carolina DMV website, Compl., ¶ 39, a record in the possession of the South Carolina DMV.⁴ The fact a web browser is used as an intermediary to send information from the DMV website to Meta’s website, facebook.com, does not change the fact the initial source of the information was a record in the possession of the DMV.

The DPPA’s private right of action does not say Meta’s liability turns on obtaining or using personal information from a motor vehicle record delivered by the state DMV itself. 18 U.S.C. § 2724(a). Meta violates the law when it “knowingly obtains ... or uses personal information, from a motor vehicle record, for a purpose not permitted.” *Id.* Indeed, a person can still say he or she “obtains and uses” shoes from the shoe store even if the shoe store employs a

³ The word “came” is found nowhere in the text of the Driver’s Privacy Protection Act. *See* 18 U.S.C. §§ 2721-25. Meta fails to cite a single case interpreting the DPPA to require the information “come” from the State DMV; its use of the word only obfuscates the relevant inquiry.

⁴ To the extent Meta tries to argue that the “initial source” of the Facebook ID number is Facebook because Facebook assigns these numbers to its users, it would be missing the mark. When *Andrews* speaks of the “initial source” of a first and last name in a license, it is not referring to the family member that made the name, God, or the Big Bang. Instead, it is referring to the chain of custody to that information, and asking whether the chain begins with a record that is presently maintained by the DMV. *Andrews*, 932 F.3d at 1260 (noting that the chain in that case began with a license that was presently in “the possession of an individual, not the DMV that issued it”). That something or someone else may have independently created the information at some point in the past is of no consequence.

mailman to deliver the person his or her shoes. The fact the transmission here occurs online makes no difference under the DPPA's plain language. To hold otherwise would give defendants a license to violate the law whenever they wish by using an agent to deliver them the information.

On this point, *Senne v. Village Of Palatine, Illinois*, 695 F.3d 597 (7th Cir. 2012) is instructive. In *Senne*, the Seventh Circuit reversed an order granting a motion to dismiss a DPPA claim based on a police department placing a parking ticket containing the plaintiff's name and other personal information on a car's windshield. *Id.* "Various pieces of personal information, obtained by the Village [police department] from a database originating with the Illinois Department of Motor Vehicles, were printed on the citation." *Id.* at 599 (emphasis added); *accord Andrews*, 932 F.3d at 1260 (focusing on the "initial source"). "The initial disclosure by the Illinois DMV to the police department," was permissible. *Id.* at 602. But the defendant in *Senne* argued "the secondary act of the Village's police department in placing the citation, which included Mr. Senne's personal information, on the windshield," was not actionable under the DPPA. 695 F.3d at 602. The Seventh Circuit rejected this argument, noting that the DPPA's "use of the term 'disclose' and of 'redisclose'" showed "that Congress intended to include within the statute's reach ... the placement of the printed citation on Mr. Senne's windshield." *Id.* at 602-03. In other words, the Seventh Circuit held that the presence of an intermediary – *i.e.*, the police officer, who printed and placed the ticket on the windshield – was not relevant so long as the initial source of the plaintiff's name and other personal information was a record in the DMV's possession. Likewise, here, the initial source of the cookies containing the Facebook ID numbers was the South Carolina DMV website, Compl., at ¶ 39, which is a record in the DMV's

possession. Plaintiff's web browser – like the police officer in *Senne* – was simply the intermediary that delivered the cookies containing Facebook ID numbers to Meta.

None of the cases Meta cites support its cause because, in those cases, the initial source of the information was not the state DMV. In *Andrews*, it was drivers' licenses in the possession of drivers. And in *Garey v. James S. Farrin, P.C.*, it was “car accident reports” in the possession of “law enforcement agencies.” 35 F.4th 917, 919-20 (4th Cir. 2022). Here, in contrast, the initial source of the personal information is the South Carolina DMV website, a record in the possession of the South Carolina DMV. As the DPPA's legislative history makes clear, this is the kind of disclosure the DPPA was meant to regulate.

4. Mr. Keogh Gives Meta Fair Notice What His Claim Is

Meta gripes that Mr. Keogh “never alleges that he visited any particular webpage or clicked any particular button... Instead, he simply notes generally that he visited the DMV's website ‘to complete various kinds of online business with the DMV’ and ‘conduct other private business with the South Carolina DMV.’” MTD at 5; see also *id.* at 7. But Mr. Keogh need not publicly disclose his private affairs in a public court filing just to state his claim. Indeed, the whole point of Driver's *Privacy* Protection Act is to protect this information from disclosure. Mr. Keogh need not waive his rights under the law just to bring a claim under it. That the plaintiff in *Gershzon* publicly revealed in an unredacted court filing that “he visited the California DMV's website ‘to apply for a disabled parking placard,’” MTD at 7, is his prerogative, but is nowhere near the applicable pleading standard. All that is required is “‘a short and plain statement’ ... ‘giv[ing] the defendant fair notice of what the ... claim is and the grounds upon which it rests.’” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (citation omitted); accord *Akkawi v. Sadr*, 2021 WL 3912151, at *6 (E.D. Cal. Sept. 1, 2021) (denying a motion to

dismiss DPPA case where defendants argued plaintiffs “cannot show that Defendants accessed DMV records of these 6 Plaintiffs”). In plain English, Mr. Keogh should not be forced to publicly reveal his disability status – or similar private information – to state a legal claim for relief in a case brought pursuant to a *privacy statute*.

As alleged, this class action rests on Meta “surreptitiously tracking South Carolinians’ permanent disability placard renewals, new car registrations, and other activity on the South Carolina State Department of Motor Vehicles (‘DMV’) website, at <https://scdmvonline.com/>, down to the very last button click.” Compl., ¶ 1. Meta knows how its own tracking Pixel works, but even if it did not, the Complaint explains that too. *Id.* ¶¶ 13-19. The Complaint also uses eleven figures showing what information is sent from the South Carolina DMV website to Meta and how Meta uses the information it receives to deliver targeted advertisements to South Carolinians. *Id.* ¶¶ 20-42, Figs. 1-11. What is more, “Meta confirms that it matches activity on the South Carolina DMV website with a Facebook user’s profile. Meta allows users to download their ‘off-site activity,’ ... The off-site activity report confirms Meta identifies a driver’s activities on the South Carolina DMV website.” *Id.* ¶ 40; *see also id.*, Fig. 11. So Meta can look through its own vast trove of off-site activity data to figure out what webpages Mr. Keogh visited.

So “the complaint, taken as a whole, ‘pleads facts ... showing unlawful behavior, [and] give the defendant fair notice of what the claim is.’” *Reetz v. Lowe's Companies, Inc.*, No. 518CV00075KDBDCK, 2019 WL 4233616, at *3 (W.D.N.C. Sept. 6, 2019).

B. Meta Cannot Collect And Use Personal Information For Targeted Advertising Without Obtaining Express Consent

Meta’s next argument, that it has obtained or used Mr. Keogh’s personal information for a permitted purpose, fares no better. *See Gershzon*, 2023 WL 5420234, at *9 (“Whether Meta in fact had a permissible purpose in obtaining and using personal information from the DMV website raises factual questions to be resolved on summary judgment or at trial.”). Even still, this Court should address them now, because, even assuming Meta’s unsupported factual allegations are true, they fail as a matter of law. As Meta will raise these defenses again at a later stage of the litigation, judicial economy will be served if the Court rejects them sooner rather than later.

Meta argues that it obtained and used information from the South Carolina DMV website under the 18 U.S.C. § 2721(b)(1), (2), and (13) exceptions. MTD at 10-12. But none of those exceptions apply because Meta uses South Carolinian drivers’ personal information for direct marketing and bulk solicitation, which is strictly regulated by the (b)(12) exception’s express consent regime. *See Maracich v. Spears*, 570 U.S. 48, 66–68 (2013); Compl., ¶¶ 62-63.

The (b)(12) exception provides that personal information may be used “[f]or bulk distribution for surveys, marketing or solicitations if the State has obtained the express consent of the person to whom such personal information pertains.” 18 U.S.C. § 2721. This exception goes to one of the core motivating factors behind the DPPA’s passage: Congressional “concern related to the States’ common practice of selling personal information to businesses engaged in direct marketing and solicitation.” Compl., ¶ 4 (quoting *Maracich*, 570 U.S. at 57). “Because (b)(12) represents Congress’ decision to target the problem of bulk solicitation with the requirement of express consent, other exceptions should not be construed to interfere with this

statutory mechanism unless the text commands it.” *Maracich*, 570 U.S. at 67 (emphasis added) (narrowly interpreting of the (b)(4) litigation exception to *not* apply to attorney solicitations).

Yet Meta has impermissibly obtained and used South Carolinian drivers’ personal information for the “bulk distribution of ... direct marketing and solicitation.” “Meta owns facebook.com and generates revenue by selling advertising space on Facebook, and other applications it owns, like Instagram.” Compl., ¶ 14. Meta obtains and uses South Carolinian drivers’ personal information “to deliver targeted advertisements to drivers on its social media platforms. This includes advertisements on Instagram for services that are ancillary to driving, such as roadside assistance services.” *Id.* ¶ 42. The Figure below, for example, “shows a driver receiving a AAA ad telling them that by joining, they can ‘skip the trip to the DMV’ on their Instagram account (owned by Meta) after visiting the South Carolina DMV website.” *Id.*



Compl., Fig. 12.

The development of new internet tracking technologies – like the Meta Tracking Pixel – has not made Congress’s concern less relevant, but more so. “Direct marketing and solicitation present a particular concern not only because these activities are of the ordinary commercial sort but also because contacting an individual is an affront to privacy even beyond the fact that a large number of persons have access to the personal information.” *Maracich*, 570 U.S. at 67.

Subsection (b)(12) implements an important objective of the DPPA – to restrict disclosure of personal information contained in motor vehicle records to businesses for the purpose of direct marketing and solicitation. The DPPA was enacted in part to respond to the States’ common practice of selling personal information to businesses that used it for marketing and solicitations. Congress chose to protect individual privacy by requiring a state DMV to obtain the license holder’s express consent before permitting the disclosure, acquisition, and use of personal information for bulk solicitation. The importance of the consent requirement is highlighted by Congress’ decision in 1999 to change the statutory mechanism that allowed individuals protected by the Act to opt out to one requiring them to opt in.

Id. at 66–67 (internal citations omitted).

As applied here, Meta’s broad reading of the (b)(1), (2), and (13) exceptions interferes with (b)(12)’s opt-in, express consent mechanism. Meta admits that is what it hopes to achieve. *See* MTD at 10 (“Plaintiff alleges that Meta used personal information ‘to deliver targeted advertisements’ and asserts he did not provide ‘express consent’ for this, Compl., ¶¶ 62-63, but as explained below ... the second [allegation] simply asserts an incorrect legal conclusion.”)

Meta argues that the (b)(1) government function and (b)(2) motor vehicle market research exceptions apply because its “Pixel helps the South Carolina DMV ... carry out its functions” and “supports [the DMV’s] own market research activities regarding how users browse its website.” MTD at 10. *Maracich* already rejected this very same argument, holding “that acquiring petitioners’ personal information for a [legitimate] purpose does not entitle respondents to then use that same information to send direct solicitations. Each distinct

disclosure or use of personal information acquired from a state DMV must be permitted by the DPPA.” 570 U.S. at 74 (emphasis added). In other words, regardless of whatever purpose the DMV has for employing the tracking Pixel, Meta cannot then turn around and use the personal information the Pixel collects for advertising without express consent. “If the statute were to operate [the way Meta would like it to], obtaining personal information for one permissible use would entitle [defendant] to use that same information at a later date for any other purpose.” *Maracich*, 570 U.S. at 74. For example, “a lawyer could obtain personal information to locate witnesses for a lawsuit and then use those same names and addresses later to send direct marketing letters about a book he wrote.” *Id.*

Other courts in the wake of *Maracich* have thus expressly rejected defendants’ invocations of the (b)(1) and (b)(2) exceptions on precisely this ground. *Hatch v. DeMayo*, 2020 WL 5763543, at *10 (M.D.N.C. Sept. 28, 2020) (quoting the court’s prior order holding that “to the extent that [the (b)(1) and (b)(14)] exceptions allow law enforcement agencies to use or disclose Plaintiffs’ personal information, neither exception immunizes liability for Defendants’ alleged disclosure of personal information for marketing or solicitation purposes”); *Akkawi v. Sadr*, 2021 WL 3912151, at *6 (E.D. Cal. Sept. 1, 2021) (“Defendants’ efforts to invoke (b)(2) are unavailing and go well beyond this preliminary stage of testing the pleadings ... Plaintiffs include as exhibits several such solicitation letters. Defendants’ instant Motion, meanwhile, does not admit or deny accessing these databases in such a way, but speaks vaguely about other ways information can be obtained.”).

Meta also argues the (b)(13) exception applies, which permits: “use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains.” This argument readily fails because Meta cannot show it has obtained Mr. Keogh’s written consent to do anything. All Meta has done is request judicial notice of a few

webpages of its various terms and policies.⁵ None of these documents bear Mr. Keogh’s written signature or otherwise have any other indication showing Mr. Keogh affirmatively consented to anything.

Meta argues that Mr. Keogh’s consent can be implied from his use of facebook.com. *See* MTD at 11. This assertion defies the plain language of the DPPA, which provides that “‘express consent’ means consent in writing.” 18 U.S.C. § 2725(5). In other words, the terms “express consent” and “written consent” are used interchangeably in the statute. And express consent cannot be secured by implication. Indeed, the words “express” and “implied” are listed as antonyms in the dictionary. The more one ponders Meta’s argument, the less sense it makes.

Misciting this same definition in a footnote, Meta argues that “written consent includes ‘consent conveyed electronically.’” MTD at 11, n.2. The full definitional clause provides: “consent conveyed electronically that bears an electronic signature as defined in section 106(5) Public Law 106-229.”⁶ 18 U.S.C. § 2725(5) (emphasis added). The word “that” modifies the electronic written consent to mean consent secured by an electronic signature. Troublingly, Meta and its counsel (Gibson Dunn) omit the portion of this definitional clause which limits the definition of written consent to exclude the implied electronic consent Meta claims it has received here. “Sometimes lawyers and their clients engage in conduct of this sort because they are incompetent. Facebook and Gibson Dunn are not incompetent.” *In re Facebook, Inc. Consumer Priv. User Profile Litig.*, 2023 WL 1871107, at *2 (N.D. Cal. Feb. 9, 2023).

⁵ *Gershzon* denied Meta’s request to judicial notice of these very same documents because “[i]f defendants are permitted to present their own version of the facts at the pleading stage – and district courts accept those facts as uncontroverted and true – it becomes near impossible for even the most aggrieved plaintiff to demonstrate a sufficiently ‘plausible’ claim for relief.” 2023 WL 5420234, at *9 n.3 (quoting *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 999 (9th Cir. 2018)); *accord Zak v. Chelsea Therapeutics Int’l, Ltd.*, 780 F.3d 597, 606 (4th Cir. 2015) (“Consideration of extrinsic documents by a court during the pleading stage of litigation improperly converts the motion to dismiss into a motion for summary judgment ... [which] is not appropriate when the parties have not had an opportunity to conduct reasonable discovery.”).

⁶ “The term ‘electronic signature’ means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.” Public Law 106-229, § 106(5).

Worse yet, Meta's implied consent argument directly interferes with (b)(12)'s opt-in consent mechanism. "The importance of the consent requirement is highlighted by Congress' decision in 1999 to change the statutory mechanism that allowed individuals protected by the Act to opt out to one requiring them to opt in." *Maracich*, 570 U.S. at 67. The act of opting in necessarily entails some kind of affirmative action. Meta's policies are the opposite of opt-in consent. Meta infers a South Carolinian's consent from his or her passive use of facebook.com, and buried on page 61 of its privacy policy is a hyperlink for "cookies-based opt out." *See* ECF No. 19-4 at 61.

Moreover, even if Meta could imply consent, its argument still fails because none of its documents explicitly notify users that they are consenting to sensitive data collection from the DMV website – as opposed to collection from general internet surfing. After all, the DMV website is not Netflix. People do not have a choice to interact with the DMV – South Carolinians *must* visit the DMV if they want to drive a car. As courts have routinely reiterated, "consent is not an all-or-nothing proposition." *In re Google Location Hist. Litig.*, 428 F. Supp. 3d 185, 192 (N.D. Cal. 2019). And as another Court explained to Meta in another case involving its Tracking Pixel collecting medical information, after reviewing the very same policies Meta now cites:

Meta's policies do not, however, specifically indicate that Meta may acquire health data obtained from Facebook users' interactions with their medical providers' websites. Its generalized notice is not sufficient to establish consent ... "In order for consent to be actual, the disclosures must 'explicitly notify' users of the practice at issue." As the Restatement explains, "[i]n order to be effective, the consent must be to the particular conduct of the actor, or to substantially the same conduct." ... In other words, "consent to a fight with fists is not consent to an act of a very different character, such as biting off a finger, stabbing with a knife, or using brass knuckles." ... I am skeptical that a reasonable user who viewed Meta's policies would have understood that Meta was collecting protected health information. The nature of the data collection that plaintiffs agreed to is akin to

the general internet browsing ... the collection of protected health information from a medical provider is a different matter entirely.

In re Meta Pixel Healthcare Litig., 647 F. Supp. 3d 778, 793-94 (N.D. Cal. 2022) (internal citations omitted). Indeed, the Court noted that Meta’s Business Tool Terms – submitted here as ECF No. 19-6 – actually undermine Meta’s implied consent argument:

This is especially true because other Meta policies (such as the Business Tool Terms) expressly provide that website developers will not share data that they “know or reasonably should know ... includes health, financial or other categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines.” Business Tool Terms at 2, see also Commercial Terms at 2 (using similar language).

In re Meta Pixel Healthcare Litig., 647 F. Supp. 3d at 794 n.9.

C. Meta’s Ignorance of the Law Is Not A Defense

Lastly, “Meta argues that ‘knowingly’ ‘requires knowledge that the defendant’s conduct satisfied all elements of the offense’ and thus that [Plaintiff] must allege that Meta essentially knew it was violating the DPPA by collecting and using personal information from the DMV website.” *Gershzon*, 2023 WL 5420234, at *9; *see also* MTD 12-13. But Meta’s radical interpretation of the DPPA abrogates “the ‘common maxim, familiar to all minds, that ignorance of the law will not excuse any person, either civilly or criminally.’” *Jerman v. Carlisle, McNellie, Rini, Kramer & Ulrich LPA*, 559 U.S. 573, 581 (2010) (citing *Barlow v. United States*, 7 Pet. 404, 411 (1833)) (holding that a defendant cannot assert a defense based on its “mistaken interpretation of the legal requirements of” another federal statute).

As *Gershzon* pointed out, “Meta does not cite any cases interpreting the DPPA which hold that ‘knowingly’ applies to all three elements of the statute.” 2023 WL 5420234, at *10. To the contrary, “District courts have held that as a matter of statutory construction, the

‘knowingly’ requirement applies to the first element of a DPPA claim.” *Id.* (collecting cases). And every Circuit Court interpreting the DPPA’s “knowingly” requirement has held that “[v]oluntary action, not knowledge of illegality or potential consequences, is sufficient to satisfy the mens rea element.” *Senne*, 695 F.3d at 603; *Pichler v. UNITE*, 542 F.3d 380, 396–97 (3d Cir. 2008); *United States v. Hastie*, 854 F.3d 1298, 1305 (11th Cir. 2017).

Here, Mr. Keogh alleges exactly that: he alleges that Meta knowingly and voluntarily obtained and used information it collected from the South Carolina DMV website. “Defendant knew it would obtain [personal] information from the South Carolina DMV website because it allowed the South Carolina DMV to set its website as a place that hosts the Meta Tracking Pixel. Defendant knowingly used the personal information it obtained from the South Carolina DMV website to deliver targeted advertisements to Plaintiff and Class members.” Compl., ¶¶ 61-62.

Meta argues that its Pixel is a “commonly used tool” and the complaint “does not show Meta knew the South Carolina DMV would use that tool to send protected information.” MTD at 12. But Meta knows its Pixel invariably sends facebook.com the Facebook ID numbers of users visiting other websites, like the DMV. *See, e.g.*, Compl., Fig. 16. Likewise, in *Hastie*, a state employee facing a criminal conviction for disclosing drivers’ email addresses in violation of the DPPA claimed “that the rule of lenity should apply because she did not know email addresses were covered by the Act.” 854 F.3d at 1305. The Eleventh Circuit rejected this argument and put her behind bars because “the Act does not require knowledge that such disclosure is illegal.” *Id.* Worse yet, Meta knew it would be receiving this protected information from the South Carolina DMV website. After all, Meta “introduced first-party cookies in 2018 to allow its tracking Pixel to circumvent improvements in how web browsers block third-party

cookies ... a first party cookie became another default [Meta Tracking] Pixel setting in or around October 2018.” Compl., at ¶ 37; *see also Gershzon*, 2023 WL 5420234, at *2.

Meta argues that “the only affirmative action Meta arguably takes is designed to *avoid* receipt of protected information.” That is patently false. First, Mr. Keogh alleges that Meta affirmatively “deliver[s] targeted advertisements to Plaintiff and Class members,” based on the information it collects from the DMV. Compl. ¶ 62. Indeed, the complaint shows how users start receiving AAA ads telling them to “skip the trip to the DMV” on Instagram shortly after visiting the DMV website. *Id.* at ¶ 42. These ads did not pop up on users’ accounts by coincidence. Second, Meta affirmatively encourages website operators, like the South Carolina DMV, to implement its Meta Tracking Pixel so it can sell “advertising space on Facebook, and other applications it owns, like Instagram.” *Id.* at ¶ 14, *see also id.*, ¶¶ 15-19. “It’s almost as if Facebook and Gibson Dunn [are] trying to gaslight their opponents, not to mention the Court.” *In re Facebook*, 2023 WL 1871107, at *1.

Meta even contends that the *Gershzon* court “did not engage with these issues.” MTD at 13. But it is Meta that is not engaging with the consequences of its actions by burying its head in the sand. Meta repeatedly notes its Meta Tracking Pixel is a “commonly used tool.” But so are guns. No court in America would absolve a gunrunner from liability for selling guns to drug cartels because he deliberately remains ignorant of what his “commonly used tools” are being used for. And yet that is precisely what Meta has done with its Tracking Pixel.

Meta has made its Meta Tracking Pixel available to any and every website that asks for it; no questions asked. Indeed, its “commonly used tool” has been used to surveil the most private parts of Americans’ daily lives in flagrant violation of multiple state and federal privacy laws. Meta’s commonly used tool collects Americans’ medical diagnoses on online medical provider

portals, *In re Meta Pixel Healthcare Litig.*, 22-cv-03580-WHO (N.D. Cal.), their personal finances on tax filing preparation websites, *In re Meta Pixel Tax Filing Cases*, Case No. 22-cv-07557-PCP (N.D. Cal.), the things they buy on Walmart, *Cappello v. Walmart Inc.*, Case No. 18-CV-06678-RS (N.D. Cal.), the news they read, *Ambrose v. Bos. Globe Media Partners LLC*, Case No. CV 21-10810-RGS, (D. Mass.), and even the videos they watch on multiple streaming services, *McCoy et al. v. AMC Networks, Inc.*, 1:23-cv-00441 (S.D.N.Y.). “The allegations against Meta are troubling [and] plaintiffs raise potentially strong claims on the merits.” *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 783. Meta cannot disclaim knowledge by citing to its terms. “The willful blindness instruction allows the jury to impute the element of knowledge to the defendant if the evidence indicates that he purposely closed his eyes to avoid knowing what was taking place around him.” *United States v. Schnabel*, 939 F.2d 197, 203 (4th Cir. 1991).

III. CONCLUSION

For the foregoing reasons, Meta’s motion should be denied in its entirety.

Dated: December 8, 2023

/s/ Blake G. Abbott
 Blake G. Abbott (Fed ID #13354)
 Paul J. Doolittle (Fed ID #6012)
POULIN | WILLEY |
ANASTOPOULO, LLC
 32 Ann Street
 Charleston, SC 29403
 Tel: (803) 222-2222
 Email: pauld@akimlawfirm.com
 blake@akimlawfirm.com

BURSOR & FISHER, P.A.

Neal J. Deckant (*pro hac vice app. forthcoming*)
 Stefan Bogdanovich (*pro hac vice app. forthcoming*)

1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ndeckant@bursor.com
sbogdanovich@bursor.com

Attorneys for Plaintiff

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on 8th day of December 2023, a copy of Plaintiff's Opposition to Defendant's Motion to Dismiss was electronically served via this Court's Electronic Case Filing (ECF) System on all counsel of record.

/s/Blake G. Abbott